MENTONE GIRLS' GRAMMAR

Privacy Policy

Help for non-English speakers.

If you need help to understand this policy, please contact the Head of Senior or Head of Junior School.

Mentone Girls' Grammar acknowledges the Bunurong People of the South-Eastern Kulin Nations for their connection to land, sea and community, and for their custodianship of the land on which we live, learn and work. We pay our respects to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander people today.

Purpose

This Privacy Policy sets out how Mentone Girls' Grammar (the School) collects, uses, stores, discloses, stores and protects personal, sensitive and confidential information and how we comply with the Australian Privacy Principals contained in the Privacy Act 1988 (*Cth*) (APPs) as well as the requirements of the Health Records Act 2001 (Vic).

It also outlines the School's approach to data breaches, including notifiable breaches under the Notifiable Data Breaches (NDB) scheme.

By sharing personal information with the School, you agree to the collection, use and disclosure of your personal information in accordance with this Privacy Policy and any other arrangements that apply between the School and you.

Scope

This Privacy Policy applies to all personal, sensitive and health information collected, used, stored or disclosed by the School in any form, including information relating to students (current, prospective and former), parents, guardians and carers, staff, volunteers, contractors, homestay providers, school council members, job applicants, alumni, donors and visitors. It covers all aspects of the School's operations such as enrolment, administration, student records, teaching and learning, wellbeing programs, child safety, employment and human resources, financial and fundraising activities, and the use of digital platforms and technologies. All members of the School community are expected to manage personal information in accordance with the Australian Privacy Principles and this policy.

Australian Privacy Principles (APPs)

The Australian Privacy Principles (APPs) are a set of 13 legally binding standards under the *Privacy Act 1988 (Cth)* that regulate how organisations, including schools, collect, use, store, protect, and disclose personal information. They provide a framework for transparent and responsible information management, covering areas such as open communication about privacy practices, how information is collected, the quality and security of the data held, when it may be shared (including overseas), and the rights of individuals to access or correct their information. The APPs apply to all entities governed by the Privacy Act and are designed to ensure privacy protections remain clear, consistent, and adaptable across a wide range of contexts.

MENTONE GIRLS' GRAMMAR

Privacy Officer

The School has a Privacy Officer who can be contacted about this Policy or about your personal information by:

Emailing: privacy@mentonegirls.vic.edu.au

Calling: 03 9581 1200

Writing to our Privacy Officer at: 11 Mentone Parade, Mentone, 3194

Our Privacy Officer is **Mr Stuart Hergt, Director of Business Operations**.

Contact can be anonymous (i.e. without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive.

Personal Information the School Collects and Holds

Definitions

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Personal information includes sensitive information about a person and their health information.

Sensitive information is personal information that includes information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a professional, trade or political association or union, religious beliefs or affiliations, philosophical beliefs, sexual orientation or criminal record.

Health information is information or an opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services, or a health service provided to the individual, currently or in the future.

The School will only collect sensitive information and health information where it is reasonably necessary for, or directly related to, our functions and activities as an independent Anglican day school in Victoria and either:

- The individual has consented; or
- The School is required or authorised by or under law, including under the APPs, to collect such information.

Personal information collected and held

The kinds of personal information that the School collects and holds about particular individuals includes:

- **Students and prospective students:** names, date of birth, addresses and other contact details, next of kin, identity documents (such as birth certificates), gender, photographs and video images, health information (such as medical records, immunisation status, individual healthcare plans, counselling and psychology reports, prescription and other pharmaceuticals being taken, dietary requirements), information concerning special needs or disability, religion, government related identifiers, nationality, country of birth, languages spoken at home.
- **Parents/guardians and prospective parents/guardians** names, addresses and other contact details, marital status, court orders affecting the parents/guardians and students, identity documents and financial information, photographs, religion, government related identifiers
- **Prospective staff:** names, addresses and other contact details, marital status and next of kin, identity documents, photographs, Working with Children clearances, VIT registration details, National Police Record checks, health information, personal references, employment history, qualifications

- **Volunteers and Contractors** names, addresses and other contact details, personal references, Working with Children clearances, National Police Record checks, employment history, qualifications
- Other persons who engage with the School names, addresses and other contact details, such as other personal information necessary in the circumstances.

Employee Records
Employee records are generally exempt from the Australian Privacy Principles (APPs) when used for employment-related purposes. The APPs apply only if the information is used for purposes unrelated to the employment relationship.

Workplace laws require certain employee information to be maintained. For questions about staff records or access, contact the Director of Human Resources.

Why do we collect personal information

Students and Families

Our School collects information about students and their families for the primary purpose of:

- Educating students and providing them access to our co-curricular activities and programs and facilities.
- Supporting students' social and emotional wellbeing, health and to fulfil legal requirements and obligations, including to:
    - Take reasonable steps to mitigate or remove risks of harm to students, staff and visitors (duty of care).
    - Make reasonable adjustments for students with disabilities (anti-discrimination law).
    - Provide a safe and secure workplace (occupational health and safety law) and to provide education, pastoral care, extra-curricular and health services.
    - Satisfy our legal obligations including our duty of care, mandatory reporting and child protection obligations.
- Enabling our School to:
    - Communicate with parents/ guardians about students' schooling matters and celebrate the efforts and achievements of students.
    - Keep parents informed as to School community matters through correspondence, newsletters and magazines and E-News.
    - Maintain the good order and management of our School.
    - Ensure the effective management, resourcing and administration of our School.
    - Fulfil statutory functions and duties.
    - Plan, fund, monitor, regulate and evaluate the Schools' policies, services, functions, school administration including for insurance purposes.
    - Assist improvement of our daily operations including training our staff; systems development; developing new programs and services; undertaking planning, research and statistical analysis.
    - Comply with reporting requirements.
    - Investigate incidents in the School and/or respond to any legal claims against the School or its staff.
    - Support community-based causes and activities, charities and other causes in connection with the Schools functions or activities.
    - Employ staff and allocate resources.

- Engage volunteers and contractors.
- Distribute promotional and fundraising activities within the School.
- Support the activities of School Associations; Friends of the Willow, Old Girls' Club including Reunions.

In some cases, if the information requested is not provided, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity. Importantly, the School cannot exercise an appropriate duty of care if you do not provide information relevant to your child's care.

Staff, Volunteers, Homestay Providers, Contractors, School Council members and Job Applicants

The School collects information regarding these groups:

- To assess applicants' suitability for employment or volunteering.
- To assess the suitability and expertise of School Council members to serve on the School Council.
- To assess the suitability of a contractor or third party to provide services within the School.
- To assess the suitability of a Homestay Provider to provide accommodation services to our Overseas Students.
- To administer employment, contractor or volunteer placement.
- For insurance purposes, including public liability and Workcover.
- To fulfil various legal obligations, including employment and contractual obligations, VRQA Minimum Standards, ESOS requirements, Child Protection and Safety obligations, Occupational Health and Safety law and to investigate incidents.
- To respond to legal claims against our School.

In some cases, if the information requested is not provided, the School may not be able to assess an individual's suitability for engagement, or continuing engagement, by the School, or to be able to properly and safely administer the individual's engagement, thereby leading to the engagement being terminated.

In relation to volunteers, if the information requested is not provided, the School may not be able to assess an individual's suitability to undertake, or continuing to undertake, volunteer work for the School, or to be able to properly and safely administer the individual's engagement as a volunteer, thereby leading to the engagement being terminated.

How we collect personal information

How the School collects personal information will largely be dependent upon whose information we are collecting. If it is reasonable and practical to do so, we collect personal information directly from the individual.

Our most common methods of collection are:

Forms and personal contact

The collection of personal information from parents/guardians is generally through the enrolment application process (by using specifically designed forms such as Enrolment Forms or a Health Information Disclosure Form) or during the course of a student's enrolment, by means such as, face to face meetings and interviews, telephone, online meetings, from correspondence (in writing, by email or other electronic means).,

The School also collects personal information about its students during their enrolment and attendance at the School, through means such, as face to face meetings and interviews, from correspondence (in writing, by email or other electronic means), while undertaking courses and other School activities.

Personal information about prospective employees, volunteers and contractors is collected through the recruitment or selection process, during face-to-face meetings and interviews, by telephone, from past employers and referees, and during the School year by way of forms or online as required for the School to

undertake its educational functions and activities.

Online Tools
At times, the school may require collecting personal information through online applications and other software used by the School such as emails, mConnect, Consent2Go and other platforms.

The personal information of visitors that will be collected at Reception through the Schools visitor management system includes their name, address and contact details, photograph and employer or contractor details.

Surveillance
The School may also collect personal information through lawful security surveillance activities such as by use of CCTV security cameras and through monitoring the use of its email and IT systems.

How we store Personal and Confidential information

The School is committed to safeguarding all personal, sensitive, and confidential information in its care. We take reasonable steps to protect this information from misuse, loss, unauthorised access, modification, or disclosure, and apply consistent security measures across both digital and physical environments. Personal information is stored in a range of formats, including secure databases, hard-copy files, school-issued devices (laptops, mobile phones, cameras and other recording devices), and in limited circumstances, staff personal devices authorised for work use. Access to information is strictly controlled on a need-to-know basis, with role-based security permissions applied across School systems.

To ensure ongoing protection, the School implements layered security measures, including:

- restricting database access using security profiles aligned with staff roles
- requiring staff to maintain the confidentiality of personal passwords
- storing sensitive printed information in locked filing cabinets located in secure locations
- using physical security protections across School buildings and grounds
- maintaining ICT security systems, policies, and procedures to safeguard data stored on School networks
- applying HR policies covering confidentiality, document handling, and appropriate technology use
- conducting due diligence on all third-party service providers, including cloud service providers, to ensure they follow privacy obligations comparable to the Australian Privacy Principles.

Personal information that is no longer required is securely destroyed, deleted, or de-identified in accordance with the Public Records Office of Victoria guidelines and the School's Records Management Policy.

Third Party Data Security Arrangements

Mentone Girls' Grammar takes reasonable steps to ensure that any third-party service provider accessing or handling personal information does so securely and in compliance with Australian Privacy Principle 11. APP 11 requires organisations, including schools, to protect personal information from misuse, interference, loss, and unauthorised access or disclosure.

Third-party providers engaged by the school must implement appropriate technical and organisational safeguards such as secure storage, access controls, and privacy-aligned processes, and may only collect, use, or disclose personal information for authorised educational purposes. Providers are required to maintain data security standards consistent with contractual privacy obligations, notify the school of any unauthorised disclosure or breach, and ensure personal information is returned or securely destroyed when no longer required.

Personal Information of Students

The Privacy Act does not differentiate between adults, children and young people and does not specify an age at which individuals can make their own decisions with respect to their personal information.

At Mentone Girls' Grammar we take a commonsense approach to dealing with a student's personal information and generally will refer any requests for personal information to a student's parents/guardians. We will treat notices provided to parents/guardians as notices provided to students.

There may also be occasions where parents/guardians are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on their privacy or on the privacy of others or result in a breach of the Schools' duty of care to the student, or where government agencies are involved.

Students may also attempt to claim a right to prevent disclosure of personal information to a parent/guardian, such as their School Report. Situations where a student makes a request that personal information (particularly sensitive information) not be disclosed to parents/guardian will be dealt with on a case-by-case basis and will involve the Privacy Officer and School Principal.

Consent

Mentone Girls' Grammar will treat consent provided by parents/guardians as consent provided by a student when collecting or using personal information and images of that student.

The School is cognisant of the fact that children and young people do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with students who are mature minors and especially when dealing with sensitive information), it may be appropriate to seek and obtain consent directly from students. The School also acknowledges that there may be occasions where a student may give or withhold consent with respect to the use of their personal information independently from their parents/guardians.

Parents/ guardians and students (where applicable) are required to provide the School consent at the commencement of each academic year to use images of their child throughout the year.

Additional specific consent may also be requested if the School would like to use or share images of their child for other purposes than those specified in the annual consent form.

Privacy and the School Community

The School community consists of staff, students, parents/carers, alumni, members of the community, other Schools, benefactors and other stakeholders. Mentone Girls Grammar has implemented the following procedures to comply with the APPs when information is shared in the School community.

School Directories

The School uses directories and class lists, which contain the names, contact details and other information of students and their parents/guardians. The School will obtain the consent of parents/guardians, and students if they have capacity to consent, to place their details in the School Directory or class list. Parents/guardians and students are also notified about these practices through our Collection Notices.

School Publications

Publications such as eNews and school magazines may contain personal information obtained from the individual or from external sources. Sensitive information (such as health information) will not be included in publications without specific consent.

School Libraries/Exhibitions

Where the School intends to include personal information in a library/exhibition, the student and their parents/ guardians will be notified of the planned use and the nature of the disclosure. Sensitive information (such as health information) will not be included without consent.

Disclosing Information to Other Schools

Information will not usually be passed on to other schools without prior consent of the individual to whom it belongs. However, information may be disclosed if it is for the primary purpose for which the information was collected or falls within a permitted secondary purpose.

Disclosure for purposes other than the primary purpose

Privacy Principle 2.1 states that the use and disclosure for a purpose other than the primary purpose of collection is permissible if Mentone Girls' Grammar reasonably believes that the use or disclosure is necessary to lessen or prevent: (i) a serious and imminent threat to an individual's life, health, safety or welfare; or (ii) a serious threat to public health, public safety, or public welfare. This exemption covers cases where a critical incident has arisen and allows relevant individuals to make the disclosure required to progress the coordinated effort for the care of the individual.

Sending Information overseas

The School may use cloud-based service providers and other third-party platforms to store and manage information. Where personal information is disclosed or stored overseas:

- reasonable steps are taken to ensure compliance with the APPs
- providers are contractually required to safeguard personal information
- parents/guardians will be informed where practicable.

It is not practicable to specify in this policy the countries to whom the School is likely to disclose personal information, as disclosure relies upon decisions of the School from time to time in relation to the location and data-hosting arrangements of third-party service providers.

Unsolicited Personal Information

If the School receives unsolicited personal information (i.e., information not requested by the School):

- it will be assessed to determine whether it could have been lawfully collected under the APPs
- if not required, it will be securely destroyed or de-identified.

The School will destroy information in a secure manner by either shredding it or disposing of it in our secure disposal bins that are placed around the School.

Access of personal information

Individuals have the right to request access to the personal information the School holds about them, and to request corrections where information is inaccurate, incomplete, or out of date. Requests should be made in writing to the School's Privacy Officer.

There are some exceptions where the School may refuse to provide an individual with access to their personal information, including to the extent that:

- Giving access would have an unreasonable impact on the privacy of others.
- Giving access would be unlawful.
- Denying access is required or authorised by or under an Australian law, court or tribunal order.
- Giving access would be likely to prejudice an enforcement related activity conducted by an enforcement body, such as Victoria Police.

If the School refuses to provide you with access to your personal information, we will provide you with written notice explaining the reasons for refusal and the means available to complain about the refusal.

Accuracy and Correction

The School takes all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up to date, including if requested by an individual to correct any personal information about them.

These steps include ensuring that the personal information is accurate, complete and up to date at the time of collection and when using or disclosing the personal information. We maintain and update personal information when we are advised by individuals or when we become aware through other means that their personal information has changed. It is your responsibility to contact the school if any of the details you have provided change. You should also contact the school if you believe that the information we have about you is not accurate, complete or up to date.

If the School has reason to refuse a request to correct the personal information of an individual, it will give the individual written notice of the reasons for the refusal and the mechanisms available to complain about the refusal.

To make a request to access or update any personal information the School holds about you or your child, please contact the School Privacy Officer in writing. The School may require you to verify your identity and specify what information you require. The School may also charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Data Breaches and Notifiable Breaches

A privacy/data breach is when personal information held by the School is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Privacy/data breaches can occur because of malicious attacks, accidents or human error.

The School recognises that the personal information it holds — including sensitive health, wellbeing, financial and academic information about students, families, and staff — must be protected against loss, misuse, and unauthorised access.

A data breach occurs when personal information held by the School is:

- Lost (e.g. a misplaced laptop, USB drive, or paper file containing personal records),
- Accessed without authorisation (e.g. a cyber-attack, phishing scam, or an unauthorised staff member viewing records),
- Disclosed without authorisation (e.g. personal details sent to the wrong parent or posted publicly), or
- Subject to misuse or interference (e.g. deliberate improper use by an employee or third-party service provider).

In the event of a privacy/data breach, prompt remedial action is required. In the first instance, it should be immediately reported to the Privacy Officer who will determine the appropriate action.

Notifiable Data Breaches (NDB) Scheme

Under the *Privacy Act 1988 (Cth)*, if a data breach is likely to result in serious harm to an individual (or group of individuals), the School must take additional steps in line with the Notifiable Data Breaches (NDB) scheme:

Assessment

The School will promptly investigate the suspected breach to determine:

- What personal information has been affected.
- Who has been impacted (e.g. students, parents, staff).
- The likelihood of serious harm (such as financial fraud, identity theft, reputational harm, or safety risk).

Notification

If serious harm is likely, the School must notify:

- The affected individuals (or parents/guardians if the individual is a student).
- The Office of the Australian Information Commissioner (OAIC) via an eligible data breach statement.

Notifications will include:

- A description of the breach.
- The kinds of information involved.
- Steps the School is taking to contain and address the breach.
- Guidance for individuals on how they can protect themselves.

Containment and Remediation

Immediate steps will be taken to limit the impact of the breach, such as:

- Resetting accounts or passwords.
- Working with IT providers to shut down unauthorised access.
- Recovering lost files where possible.
- Providing additional support to affected families (e.g. guidance on credit monitoring or identity protection).

Review and Prevention

- Following any breach, the School will conduct a review of policies, procedures, and systems to prevent recurrence.
- Training and awareness for staff will be strengthened as required.

Examples of Data Breaches

- A teacher emailing a student's report to the wrong parent.
- A school database being hacked, exposing medical or contact details.
- A laptop or USB with student information being lost.
- Student photos or videos being uploaded to a public platform without consent.
- A service provider (e.g. IT contractor, payment gateway) exposing parent financial details due to security practices.

Responsibilities

- All staff are responsible for handling information carefully and reporting suspected breaches immediately to the Privacy Officer.
- The Privacy Officer and Principal are responsible for coordinating the School's response, including notification and communication.
- Third-party providers (e.g. cloud services, learning management systems, payment processors) engaged by the School are contractually required to comply with privacy and security obligations.

Data Breach Procedure

If a data breach or suspected breach occurs, the School follows the procedure below:

1. **Identify and Report** – Any staff member who becomes aware of a potential breach must report it immediately to the Privacy Officer or Principal.
2. **Contain** – Immediate steps are taken to limit further access, disclosure, or loss (e.g. suspend accounts, recover emails, secure systems).
3. **Assess** – The Privacy Officer will investigate the breach within 30 days to determine:
    - The type of information affected.
    - Who is impacted.
    - Whether the breach is likely to result in *serious harm*.
4. **Notify (if required)** – If serious harm is likely, the School will:
    - Notify affected individuals (or parents/guardians for students).
    - Notify the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches (NDB) scheme.
    - Provide guidance to affected individuals on steps they can take to protect themselves.
5. **Review and Prevent** – Following resolution, the School will review policies, procedures, and systems to reduce the risk of recurrence and may conduct staff training where necessary.

Data Breach Register

To ensure accountability and compliance, the School maintains a register of Data Breaches via the school's incident reporting platform. All actual and suspected breaches are logged in this register by the Privacy Officer or Risk and Compliance Manager.

The register records:

- When and how the breach occurred.
- The type of information involved.
- Individuals affected.
- Actions taken to contain and investigate.
- Whether the NDB scheme applied.
- Notifications made to individuals and/or the OAIC.
- Remediation steps taken and lessons learned.

The incident register is reviewed regularly by the Principal and School Council (or governing body) to ensure systemic issues are identified and addressed.

By embedding the Procedure and Register into the Privacy Policy, the School ensures staff and community members understand not only their obligations but also how breaches will be handled, documented, and communicated.

Privacy Complaints

Any concerns or complaints about privacy or the handling of personal information should be directed in writing to the School's Privacy Officer. The School will:

1. Acknowledge receipt of the complaint
2. Investigate and provide a response within a reasonable timeframe
3. Take appropriate corrective action where required.

Complaints may also be made to the Office of the Australian Information Commissioner (OAIC) if you are not satisfied with the response you receive from the School - https://www.oaic.gov.au/about-us/contact-us/

Staff Training

To meet Privacy obligations, we place a strong focus on staff training, ensuring all employees understand their responsibilities when handling student, parent, and staff information. Regular training supports compliance by equipping staff to consider privacy requirements in their daily work, which is vital given the volume and sensitivity of information managed within the School.

Documents and Resources

- Child Safety Code of Conduct
- Child Safety and Wellbeing Policy
- Parent Code of Conduct
- Student Code of Conduct
- Photography and Video Images Policy
- Social Media Policy
- Responsible Use of Digital Technologies and Cyber Safety
- Complaints Handling and Resolution Policy
- Medical Records Policy
- Incident Register

References

Privacy Act 1998 (Cth)

Australian Privacy Principals (APPs)

Notifiable Data Breach Scheme

Department of Education Privacy Policy Guidelines

MENTONE GIRLS' GRAMMAR

Governance Table

Policy Number	POL-PP-003		
Policy Owner	Privacy Officer	Policy Approver	SMT/GRCC/Council
Approval Date	March 2026	Next Review	March 2028
Review frequency	Every 2 years		
Policy Management	This policy is administered by the Privacy Officer		

Revision History

Document	Review Period	Review Outcomes	Approval
POL-PP-001	23 August – December 2022	Review and Updates Legal Counsel Review	School Council Gadens
POL-PP-002	30 May 2023	Cyclical Review	Principal
POP-PP-003	October 25 – February 2026	Update to Privacy Officer Addition of Notifiable Data Breach procedures Review against changes to ELC new requirements	SMT – 18 Feb. 26 GRCC – 25 Feb. 26 Council